**DEPARTMENT OF HEALTH & HUMAN SERVICES**
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

**CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)**

Office of Information Services (OIS)
Security and Standards Group (SSG)

# CMS Information Security Incident Handling Procedures

Version 1.0

March 9, 2004

# Executive Summary

The Centers for Medicare & Medicaid Services (CMS) is the Federal agency that administers Medicare, Medicaid and the State Children's Health Insurance Program (SCHIP). CMS is responsible for protecting health insurance and patient information used in the administration of CMS programs, as well as computer systems that facilitate the delivery of such services to the public.

CMS' Information System Security Program has numerous initiatives to prevent and minimize computer systems and/or sensitive data compromises. Dependencies on technology to support business functions and delivery of CMS' programs expose the operational environment to risks of accidental and intentional security breaches. Therefore, preparation and coordination to handle security incidents occurrence improve the overall security posture of the enterprise by providing a systematic process of security incident management. Roles and responsibilities are identified, and escalation procedures are defined to provide an orderly approach to incident response.

Incident response involves the following phases: preparation, detection, alert, triage, response (containment and eradication), recovery and follow-up. The goal of a systematic approach to handle security incidents is to resume system and business operations as soon as possible while preserving the incident's forensics information for further analysis and security process enhancements.

Escalation procedures are based on incidents that may occur within the CMS business environment. This covers business conducted in CMS facilities, by CMS employees and contractor personnel, as well as those contractors covered by the systems security requirements in the CMS Business Partner System Security Manual (i.e. Medicare Carriers, Fiscal Intermediaries, shared system maintainers, and data center and program safeguard contractors.)

Security incidents have been classified into five levels based on severity. They range from small numbers of system probes on internal systems to successful penetration with significant impact on operations and data compromise. The security incident severity levels from low to high are:

1. Small number of system probes or scans on external systems; isolated instances of known computer viruses easily handled by anti-virus software; loss of personal password by non-administrative system user.
2. Small numbers of system probes or scans detected on internal systems by internal addresses; unexplained increase of instances of known computer viruses easily handled by anti-virus software; security advisories/information received concerning threats to systems and potential system vulnerabilities of low or general risk, no identifiable or specific disruptive incident. All security advisories/information applicable to CMS systems will be entered at this level and be evaluated by System Technical Support.
3. Significant numbers of system probes or scans detected; penetration or denial-of-service attacks attempted with no impact on operations; instances of new computer viruses not handled by anti-virus software with limited impact on operations; security advisories/information evaluated and upgraded, involving threats to systems and potential

system vulnerabilities of a credible, elevated risk, but not specifically disruptive to CMS systems.

4. Penetration or denial-of-service attacks attempted with limited impact on operations; widespread instances of a new computer virus not handled by anti-virus software; information disclosure with some risk to privacy information or public relations impact; security advisories/information evaluated and upgraded, involving threats to systems and potential system vulnerabilities of a credible, high risk, and specifically disruptive to CMS systems.
5. Successful penetration or denial-of-service attacks detected with significant impact on operations; information disclosure with significant risk to privacy information or public relations impact; security advisories/information evaluated and upgraded, involving threats to systems and potential system vulnerabilities of an imminent, credible, severe risk, and specifically disruptive to CMS systems.

Lower severity levels will be handled by the technical staff responsible for operations and administration of the system, while management of higher severity levels will be referred to a multi-component management team for further incident level assessment, coordination and reporting.  Depending on the severity, source of the incident and policies, reports will be prepared and sent to the CMS Chief Information Officer, the Department of Health and Human Services' Information System Security Officer and other government agencies.

# Table of Contents

# 1. Introduction

## 1.1 Definition

A security incident is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of data or system availability.

## 1.2 System Security Incident Response Phases

### 1.2.1 Preparation Phase

The preparation phase is the process of establishing policies, processes, procedures and agreements covering the management and response to system security incidents such as guidelines identifying levels and responses, auditing and logging, reporting guidelines, resolution and follow-up.

### 1.2.2 Alert Phase

The alert phase is the process of learning about a potential security incident, and reporting it to generate an incident ticket. Alerts may arrive from a variety of sources including: monitoring of firewalls and intrusion detection systems, anti-virus software, threats received via electronic mail, and media reports about new threats.

### 1.2.3 Triage Phase

The triage phase involves the process of examining the information available about the situation to determine whether or not a security incident has occurred. During this phase, the incident component lead is assigned. If an incident has occurred, the nature of the incident is determined, the initial severity level is assigned and the documentation of all actions taken is initiated. This phase may also involve creating an Incident Response Team (IRT) to work on activities relating to incident handling. A decision to "pursue" or "protect" is made during this phase according to the sensitivity of the data and criticality of the operational system. If a decision to "pursue" is made, it assumes the intrusion or misuse continues as analyst(s) gather information about the malicious activity before proceeding to "protect" the system and initiate actions to discontinue the unauthorized actions as in the containment and eradication phases. In either case, protective actions will be performed on the system to safeguard data and system resources on the affected system. For higher severity level incidents, consideration is given to potential legal or public relations impacts arising from each course of action.

### 1.2.4 Response (Containment and Eradication) Phase

The response phase is the process of limiting the scope and magnitude of an incident in order to keep the incident from getting worse. Consideration is given to factors such as system backup, the risk of continuing operations, and changing passwords or access controls lists on the compromised systems and data. This phase also involves determining the cause of the incident, improving system defenses, determining system vulnerabilities and removing the cause of the incident to eliminate possibility of reoccurrence. For high severity levels, business continuity plan may be put into effect.

#### 1.2.5 Recovery Phase

The system and business process returns to full and normal operations during this phase. Actions include restoring and validating the system, deciding when to restore operations and monitoring systems to verify normal operations without further system or data compromise.

#### 1.2.6 Follow-up Phase

This phase involves developing an incident report and disseminating it to appropriate entities according to established policies; identifying lessons learned from the incident handling process including the successful and unsuccessful actions taken in response to an incident; developing recommendations to prevent future incidents and to improve enterprise security implementation.

## 2. Roles and Responsibilities

### 2.1 System User

#### 2.1.1 Description

CMS employees or contractor staff conducting CMS business functions.

#### 2.1.2 Responsibilities

- Reports security incidents to the appropriate point of contact (i.e., CMS IT Service Desk or System Technical Support as directed by the business organization).
- Works with System Technical Support in information gathering and incident determination activities.

### 2.2 CMS IT Service Desk

#### 2.2.1 Description

CMS or contractor staff which acts as the first point of contact for reported operational problems and security incidents.

#### 2.2.2 Responsibilities

- Acts as the first point of contact for system security incidents or anomalies, and records information provided by the System User, System Technical Support or Managed Security Services Provider (MSSP), depending on alert source.
- Generates security incident tickets.
- Initiates escalation procedures according to initial severity level in accordance with Technology Management Group/Lockheed Martin incident handling procedures, including paging pre-determined government/contractor staff, when appropriate, for notification, investigation, analysis, countermeasures and follow-up.

### 2.3 System Technical Support

#### 2.3.1 Description

System administrators, system maintainers, and security staff for General Support System or Major Application(s) affected by security incident, Component Information System Security Officer (Component ISSO), or External Business Partner Contact. Staff may be CMS contractor personnel operating/maintaining affected systems.

### 2.3.2 Responsibilities

- Serves as the system's focal point for security incidents for triage, response and recovery phases.
- Assigns initial severity level to security tickets.
- Prepares component-level plans and procedures to address system security incidents, in accordance with this document, and security system standard operating procedures.
- Contacts CMS IT Service Desk to report security incident or vice versa, depending on the alert source.
- Provides technical support and advice for incident handling, impact assessment, and technical system management, including actions to be taken if circumstances are not covered by standard operating procedures.
- Coordinates evaluation and categorization of security advisories/information.
- Refers security advisories/information involving high and severe risk to the IHCM Team.
- Implements changes to computer systems to minimize newly discovered vulnerabilities resulting from a security incident.
- Reports incident status/resolution information to component's management and Incident Handling Coordination and Management (IHCM) Team in accordance with this document and component's standard operating procedures.
- Updates and closes incident tickets for level 1, 2, 3 and 4 (not involving penetration) security incidents.
- Updates and transfers ticket to IHCM for level 4 (successful penetration only) and level 5 security incidents.
- Assists IHCM and Incident Response Teams in information gathering, forensics and reporting activities.
- Provides ad hoc and periodic reports on security incidents and handling of advisories to Systems Technical Support Management and SSG Management, or the IHCM.

## 2.4 Incident Handling Coordination and Management (IHCM) Team

### 2.4.1 Description

Multi-component team that provides support and management direction to high-level security incidents. Members include the Senior System Security Advisor/Security and Standards Group (SSG), Computer Security Analyst(s), the Senior Information System Security Officer (SISSO), System Technical Support Management, SSG Management, as well as the Consortium

Contractor Management Officer and CMS Project Officer for External Business Partner Contractors.

### 2.4.2 Responsibilities

- Leads incident handling coordination activities for level 4 (successful penetration) and 5 security incidents, and assesses security incident's impact and severity.
- Correlates information across multiple components' point of contact and System Technical Support.
- Coordinates information and evidence gathering, forensics effort, and follow-up activities.
- Updates and closes incident tickets for level 4 (successful penetration only) and level 5 security incidents.
- Prepares and disseminates incident updates and reports to the Chief Information Officer (CIO), and other entities, as appropriate for the security severity level.
- Specific IHCM Team role responsibilities are as follows:

#### Senior System Security Advisor/SSG Management

- Serves as liaison between the CIO, Computer Security Analysts/System Technical Support, and upper management for incident handling activities and timely reporting.
- Serves as central point of contact for required reporting of incidents, coordinating CMS response to an incident, and acting as a clearinghouse for disseminating information concerning alerts and vulnerabilities.
- Analyzes incident information and assesses security incident impact and severity.
- Informs and updates the CIO on security incidents, along with System Technical Support Management.
- Reviews and disseminates reports addressed to the CIO and other entities.

#### Computer Security Analyst (CSA)

- SSG and system staff who serve as technical liaison and support for management during incident handling.
- Coordinates incident handling activities among multiple components.
- Coordinates information and evidence gathering, forensics effort, and follow-up activities.
- Updates and closes security incident tickets.
- Prepares or coordinates preparation of security incident reports.

#### Senior Information System Security Officer (SISSO)

- Provides incident handling direction and policy clarifications.
- Assists the Senior System Security Advisor/ SSG Management.

- Directs security incident periodic statistics, trend analysis and reporting.
- Receives security advisories and disseminates them among key staff.

**<u>System Technical Support Management</u>**

- Coordinates incident handling activities within its component.
- Provides primary and alternate points of contact (POC) to the IHCM and CMS Service Desk for incident handling.
- Interacts with other System Technical Support Management in the event of more than one GSS and/or MA, managed by different components, are affected by a security incident.
- Serves as liaison between technical staff in charge of system administration and other management team members in IHCM while assisting on the incident handling decision-making process.

**<u>Consortium Contractor Management Officer and CMS Project Officer for External Business Partners</u>**

- Serves as CMS point of contract on information system security incidents for External Business Partners.
- Provides personnel and technical assistance to external business partners in support of these procedures.

## 2.5 Chief Information Officer (CIO)

### 2.5.1 Description

Responsible for overall implementation and administration of the CMS Information Security Program.

### 2.5.2 Responsibilities

- Provides overall incident handling direction for higher severity level security incidents.
- Directs decision-making activities for security incidents escalating beyond CMS boundaries and established policies.

## 2.6 Managed Security Services Provider (MSSP)

### 2.6.1 Description

Contractor staff composed of system engineers and subject matter experts that specialize on intrusion detection systems monitoring and management, firewall management, network and operating system security, malicious incident analysis and handling, and forensics analysis.

### 2.6.2 Responsibilities

- Monitors 24x7 Intrusion Detection System (IDS) data collected from MSSP-supplied IDS sensors.

- Generates alerts and warnings for possible security incidents, as CMS' intrusion detection system managers.
- Provides security advisories to CMS as security incident prevention mechanism.
- Supports information gathering, analysis and forensics activities during the incident handling process.
- Provides technical advice and support on areas of expertise, remotely or on-site.

### 2.7 Other Entities

#### 2.7.1 Description

CMS Upper Management, Department of Health and Human Services (DHHS) Information Resource Management (IRM), the Office of Inspector General's Computer Crime Unit, and the General Service Administration's Federal Computer Incident Response Capability (FedCIRC).

#### 2.7.2 Responsibilities

- Provides CMS with high-level direction and policies, and assistance for security incident response process.

### 2.8 Incident Response Team (IRT)

#### 2.8.1 Description

Logical group assembled to handle security incidents. Team membership will vary according to the severity and nature of the security incident. Team composition will be determined depending on the incident severity levels, staff identifying the security incident, System Technical Support staff and its management involvement, systems and applications affected by security incident, associated components with business and technical responsibilities on the system affected by security incident, need to involve contractors providing security services/support and/or other federal agency's staff.

#### 2.8.2 Responsibilities

- Performs a variety of incident handling activities throughout the System Security Incident Response Phases, depending on the severity level and nature of security incident.

## 3. Security Incident Information Guidelines

Security incidents are classified according to impact of operations, system criticality and the sensitivity level of the compromised data. Once the occurrence of an incident is verified, incident response phases take place in order to restore operations and mitigate system vulnerabilities. Actions taken during the incident response phases vary according to type of incident and severity level.

This section describes general guidelines for incident response phases for each incident security level category.

### 3.1 Documentation

During the incident response phases, all analysts and administrators must keep a log of all actions taken to aid in incident handling, decision-making and reporting processes. The types of information that should be logged are:

- Dates and times of incident-related phone calls.
- Dates and times when incident-related events were discovered or occurred.
- Amount of time spent working on incident-related tasks.
- The entity or people the component has contacted or who have contacted the component.
- Names of systems, programs, or networks affected by the incident.
- Impact analysis.

### 3.2 Information Release

Release of information during incident handling phases must be on a need-to-know basis. For severity levels 4 and 5, when other entities would be notified of the incident, information release must be authorized by the Senior System Security Advisor or SSG Management, in consultation with the CIO and CMS management. In the case of security incidents at External Business Partner's sites, CMS will coordinate with legal and public affairs contacts in the affected entities.

## 4. Escalation Procedures According to Severity Level

The following table summarizes each incident severity level and its description:

| Severity Level | Description |
|---|---|
| Level 1 | Small number of system probes or scans on external systems; isolated instances of known computer viruses easily handled by anti-virus software; loss of personal password by non-administrative system user. |
| Level 2 | Small numbers of system probes or scans detected on internal systems by internal addresses; unexplained increase of instances of known computer viruses easily handled by anti-virus software; security advisories/information received concerning threats to systems and potential system vulnerabilities of low or general risk, no identifiable or specific disruptive incident. All security advisories/information applicable to CMS systems will be entered at this level and be evaluated by System Technical Support. |
| Level 3 | Significant numbers of system probes or scans detected; penetration or denial-of-service attacks attempted with no impact on operations; instances of new computer viruses not handled by anti-virus software with limited impact on operations; security advisories/information evaluated and upgraded, involving threats to systems and potential system vulnerabilities of a credible, elevated risk, but not specifically disruptive to CMS systems. |
| Level 4 | Penetration or denial-of-service attacks attempted with limited impact on operations; widespread instances of a new computer virus not handled by anti-virus software; information disclosure with some risk to privacy information or public relations impact; security advisories/information evaluated and upgraded, involving threats to systems and potential system vulnerabilities of a credible, high risk, and specifically disruptive to CMS systems. |
| Level 5 | Successful penetration or denial-of-service attacks detected with significant impact on operations; information disclosure with significant risk to privacy information or public relations impact; security advisories/information evaluated and upgraded, involving threats to systems and potential system vulnerabilities of an imminent, credible, severe risk, and specifically disruptive to CMS systems. |

During the Alert Phase for all severity levels, a System User, System Technical Support, or MSSP analyst identifies and reports a potential security incident to the CMS IT Service Desk or

System Technical Support, as appropriate for the business organization, so that a security incident ticket is ultimately opened, when contacting the CMS IT Service Desk, for tracking of the incident.

During the response phases for which it leads the incident handling coordination, the IHCM may subsequently form an IRT to work on the incident response effort, as appropriate. Team membership will vary according to the severity level and the nature of the security incident.

## 4.1 Severity Level One Incident

### 4.1.1 Description

Small number of system probes or scans on external systems; isolated instances of known computer viruses easily handled by anti-virus software; loss of personal password by non-administrative system user.

### 4.1.2 Action Steps

- The CMS IT Service Desk records information provided by a System User, System Technical Support, or MSSP, and opens a ticket.
- System Technical Support verifies the occurrence of the reported security incident, determines the nature of the security incident and assigns the initial severity level. System Technical Support updates the ticket through the CMS IT Service Desk.
- System Technical Support updates the security incident ticket with evaluation and/or problem resolution information and closes the ticket with CMS IT Service Desk.

## 4.2 Severity Level Two Incident

### 4.2.1 Description

Small numbers of system probes or scans detected on internal systems by internal addresses; unexplained increase of instances of known computer viruses easily handled by anti-virus software; security advisories/information received concerning threats to systems and potential system vulnerabilities of low or general risk, no identifiable or specific disruptive incidents. All advisories/information that is not a specific incident will be entered at this level. The advisories will be evaluated and elevated, if necessary.

### 4.2.2 Action Steps

- The CMS IT Service Desk records information provided by a System User, System Technical Support, or MSSP, and opens a ticket.
- For security incidents, System Technical Support verifies the occurrence of the reported security incident, determines the nature of the incident and risk to CMS systems and assigns an initial severity level, and updates the ticket, if necessary.
- For a security advisory or notification of pending threats or possible vulnerabilities, System Technical Support, reviews advisory/information, performs a vulnerability assessment based on information in the advisory and standard operating procedures, and updates the severity level and ticket, as appropriate.

- System Technical Support contains, mitigates, and eradicates the cause of the incident, to include creating a Corrective Action Plans (CAP), as appropriate; if necessary corrects, restores and validates affected system, and updates severity level and ticket based on actions.
- System Technical Support updates the security incident ticket with problem resolution information and closes the ticket.
- System Technical Support provides reports on incidents and advisories to the IHCM, or SSG and System Technical Support Management, as appropriate.

## 4.3 Severity Level Three Incident

### 4.3.1 Description

Significant numbers of system probes or scans detected; penetration or denial-of-service attacks attempted with no impact on operations; instances of new computer viruses not handled by anti-virus software with limited impact on operations; security advisories/information evaluated and upgraded, involving threats to systems and potential system vulnerabilities of a credible, elevated risk, but not specifically disruptive to CMS systems.

### 4.3.2 Action Steps

- The CMS IT Service Desk records information provided by a System User, System Technical Support, or MSSP, and opens a ticket.
- For security incidents, System Technical Support verifies the occurrence of the reported security incident, determines the nature of the incident and risk to CMS systems and assigns an initial severity level, and updates the ticket, if necessary.
- For a security advisory or notification of pending threats or possible vulnerabilities, System Technical Support, reviews advisory/information, performs a vulnerability assessment based on information in the advisory and standard operating procedures, and updates the severity level and ticket, as appropriate.
- System Technical Support contains, mitigates, and eradicates the cause of the incident, to include creating a Corrective Action Plans (CAP), as appropriate necessary; if necessary. corrects, restores and validates affected system, and updates severity level and ticket based on actions.
- System Technical Support updates the security incident ticket with problem resolution information and closes the ticket.
- System Technical Support will provide reports on incidents and advisories to the IHCM, or SSG and System Technical Support Management, as appropriate.

## 4.4 Severity Level Four Incident

### 4.4.1 Description

Penetration or non-penetration (such as denial-of-service attacks) incidents with limited impact on operations; widespread instances of a new computer virus not handled by anti-virus software; non-penetration incidents involving information disclosure, with some risk to privacy information or public relations impact; security advisories/information evaluated and upgraded, involving threats to systems and potential system vulnerabilities of a credible, high risk, and specifically disruptive to CMS systems.

#### 4.4.2 Action Steps

- The CMS IT Service Desk records information provided by a System User, System Technical Support, or MSSP, and opens a ticket.
- For security incidents, System Technical Support verifies the occurrence of the reported security incident, determines the nature of the incident and risk to CMS systems and assigns an initial severity level, and updates the ticket, if necessary.
    - For penetration security incidents,
        - System Technical Support immediately notifies identified IHCM contacts in accordance with approved notification list.
        - System Technical Support reports incident information to IHCM to evaluate/verify incident severity level and to determine a “pursue” or “protect” strategy.
        - System Technical Support and/or MSSP provide assistance for forensics evidence gathering and analysis, and remote or on-site support, as needed.
    - For non-penetration security incidents involving information disclosure, with some risk to privacy information or public relations impact,
        - System Technical Support immediately notifies identified IHCM contacts in accordance with approved notification list.
        - System Technical Support reports incident information to IHCM to evaluate/verify incident severity level.
    - For non-penetration security incidents with limited impact on operations,
        - System Technical Support contains, mitigates, and eradicates the cause of the incident; corrects, restores and validates affected system; and updates severity level and ticket based on actions taken.
        - System Technical Support updates the security incident ticket with problem resolution information and closes the ticket.
        - System Technical Support reports incident information to IHCM, including actions taken and resolution of vulnerabilities identified, if any.
- For security advisories/information with credible, high risk, and specifically disruptive to CMS systems,
    - System Technical Support reviews advisory/information, performs a vulnerability assessment based on information in the advisory and standard operating procedures, and updates the severity level and ticket, if appropriate.
    - System Technical Support reports findings to IHCM for enterprise-wide assessment and reporting.

- For security incident and security advisory/information, the following additional steps apply:
  - IHCM gathers information from System Technical Support for incident reporting, forms IRT, if needed, and coordinates incident handling efforts if multiple systems/components are affected.
  - System Technical Support develops a Corrective Action Plan (CAP) to protect sensitive information and resolve system vulnerabilities. System Technical Support also tracks CAP and reports to IHCM after implementation.
  - If the incident involves successful penetration or information disclosure, Senior System Security Advisor, along with System Technical Support Management and SSG Management, notifies CIO of incident occurrence and impact, and issues periodic reports to the CIO, as appropriate.
  - For security incidents impacting operations, the Senior System Security Advisor or the Senior ISSO notifies the DHHS Senior Information Systems Security Officer of the security incident.
  - System Technical Support keeps IHCM abreast of incident handling actions/progress and updates the security ticket, as appropriate. Ad hoc progress reports to IHCM are issued, as required by the situation.
  - If the incident involves successful penetration or information disclosure, System Technical Support reports incident information to the IHCM, which documents resolution information, including tally of systems affected, and updates and closes incident ticket.
  - IHCM prepares and disseminates reports to the CIO and other entities, as dictated by policies and specific mandates.
- For security incidents, the following apply:
  - IHCM coordinates with Legal and Public Affairs contacts to authorize and prepare public relations statements or legal preparation of evidence, if appropriate.
  - If a violation of the law is suspected, IHCM will notify the Office of Inspector General's Computer Crime Unit and submit an incident report to FedCIRC with a copy to the DHHS Senior Information Systems Security Officer.

## 4.5 Severity Level Five Incident

### 4.5.1 Description

Successful penetration incidents or denial-of-service attacks detected with significant impact on operations; non-penetration incidents involving information disclosure with significant risk to privacy information or public relations impact; security advisories/information evaluated and upgraded, involving threats to systems and potential system vulnerabilities of an imminent, credible, severe risk, and specifically disruptive to CMS systems.

### 4.5.2 Action Steps

- The CMS IT Service Desk records information provided by a System User, System Technical Support, or MSSP, and opens a ticket.

- For security incidents, System Technical Support verifies the occurrence of the reported security incident, determines the nature of the incident and risk to CMS systems and assigns an initial severity level, and updates the ticket, if necessary.
    - System Technical Support immediately notifies identified IHCM contacts in accordance with approved notification list.
    - For penetration security incidents,
        - System Technical Support reports incident information to IHCM to evaluate/verify incident severity level and to determine a "pursue" or "protect" strategy.
        - System Technical Support and/or MSSP provide assistance for forensics evidence gathering and analysis, and remote or on-site support, as needed.
    - For non-penetration security incidents involving information disclosure, with significant risk to privacy information or public relations impact,
        - System Technical Support reports incident information to IHCM to evaluate/verify incident severity level.
    - For non-penetration security incidents with limited impact on operations,
        - System Technical Support contains, mitigates, and eradicates the cause of the incident; corrects, restores and validates affected system.
- For security advisories/information with imminent, credible, severe risk, and specifically disruptive to CMS systems,
    - System Technical Support reviews advisory/information, performs a vulnerability assessment based on information in the advisory and standard operating procedures, and updates the severity level and ticket, if appropriate.
    - System Technical Support reports findings to IHCM for enterprise-wide assessment and reporting.
- For security incidents and security advisory/information, the following additional steps apply:
    - IHCM gathers information from System Technical Support for incident reporting, forms IRT, if needed, and coordinates incident handling efforts if multiple systems/components are affected.
    - System Technical Support develops a Corrective Action Plan (CAP) to protect sensitive information and resolve system vulnerabilities. System Technical Support also tracks CAP and reports to IHCM after implementation.
    - Senior System Security Advisor, along with System Technical Support Management and SSG Management, notifies CIO of incident occurrence and impact, and issues periodic reports to the CIO, as appropriate. For security incidents impacting operations, the Senior System Security Advisor or the Senior ISSO notifies the DHHS Senior Information Systems Security Officer of the security incident.

  - System Technical Support keeps IHCM abreast of incident handling actions/progress and updates the security ticket, as appropriate. Ad hoc progress reports to IHCM are issued, as required by the situation.
  - At the discretion of the Senior System Security Advisor or the IHCM, periodic reports are issued and/or prepared for the CIO, CMS upper management and outside entities, as appropriate.
  - IHCM documents resolution information, including tally of systems affected, and updates and closes the security incident ticket.
  - IHCM prepares and disseminates reports to the CIO and other entities, as dictated by policies and specific mandates.
- For security incidents, the following apply:
  - IHCM coordinates with Legal and Public Affairs contacts to authorize and prepare public relations statements or legal preparation of evidence.
  - If a violation of the law is suspected, IHCM will notify the Office of Inspector General's Computer Crime Unit and submit an incident report to FedCIRC with a copy to the DHHS Senior Information Systems Security Officer.

## Appendix A – CMS Incident Handling Escalation and Reporting Process

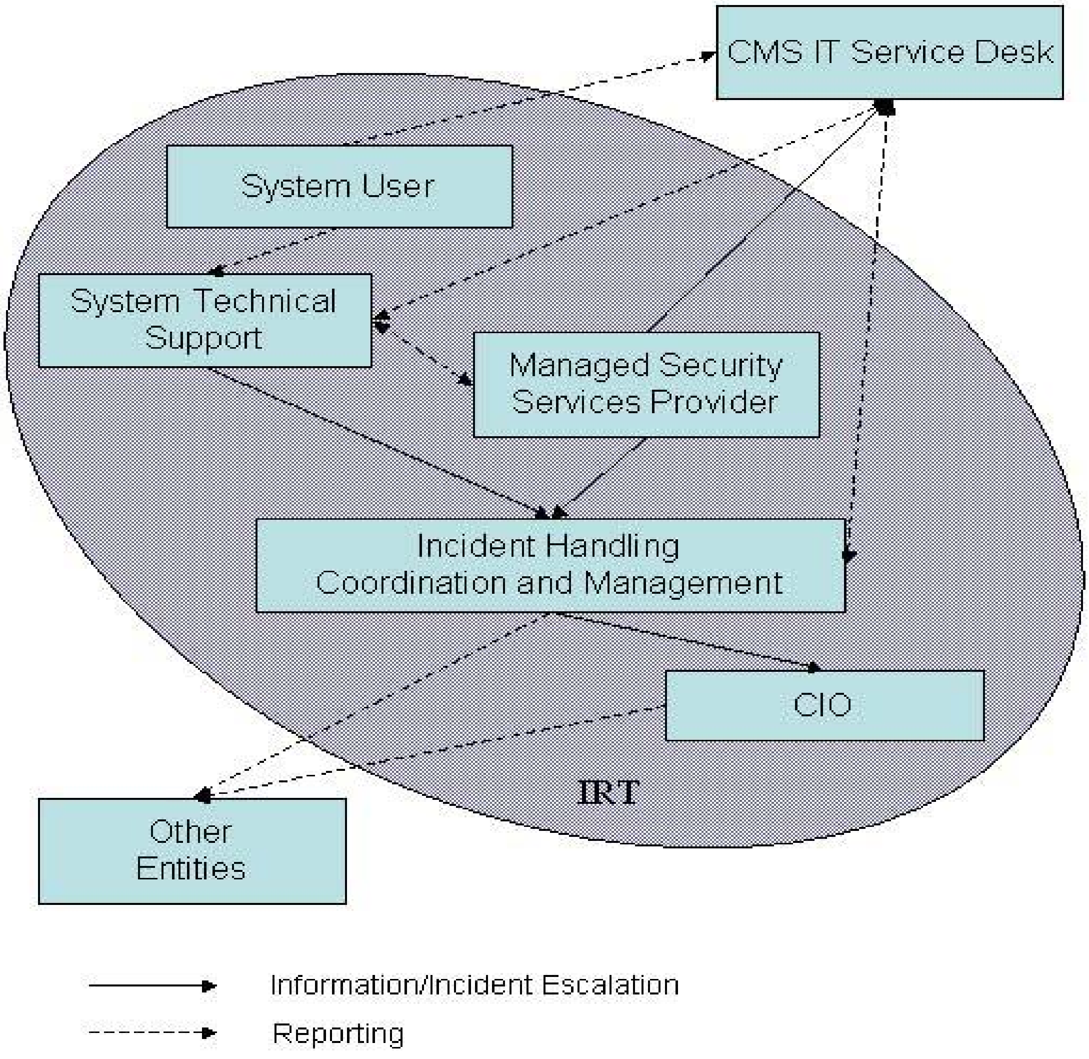
CMS IT Service Desk
System User
System Technical Support
Managed Security Services Provider
Incident Handling Coordination and Management
CIO
IRT
Other Entities
Information/Incident Escalation
Reporting

Figure A

Note: The Incident Response Team (IRT) is a logical group assembled to handle security incidents. Team membership will vary according to severity and nature of security incident.

# Appendix B – Escalation Process by Severity Level

## System Security Incident Handling Action Steps

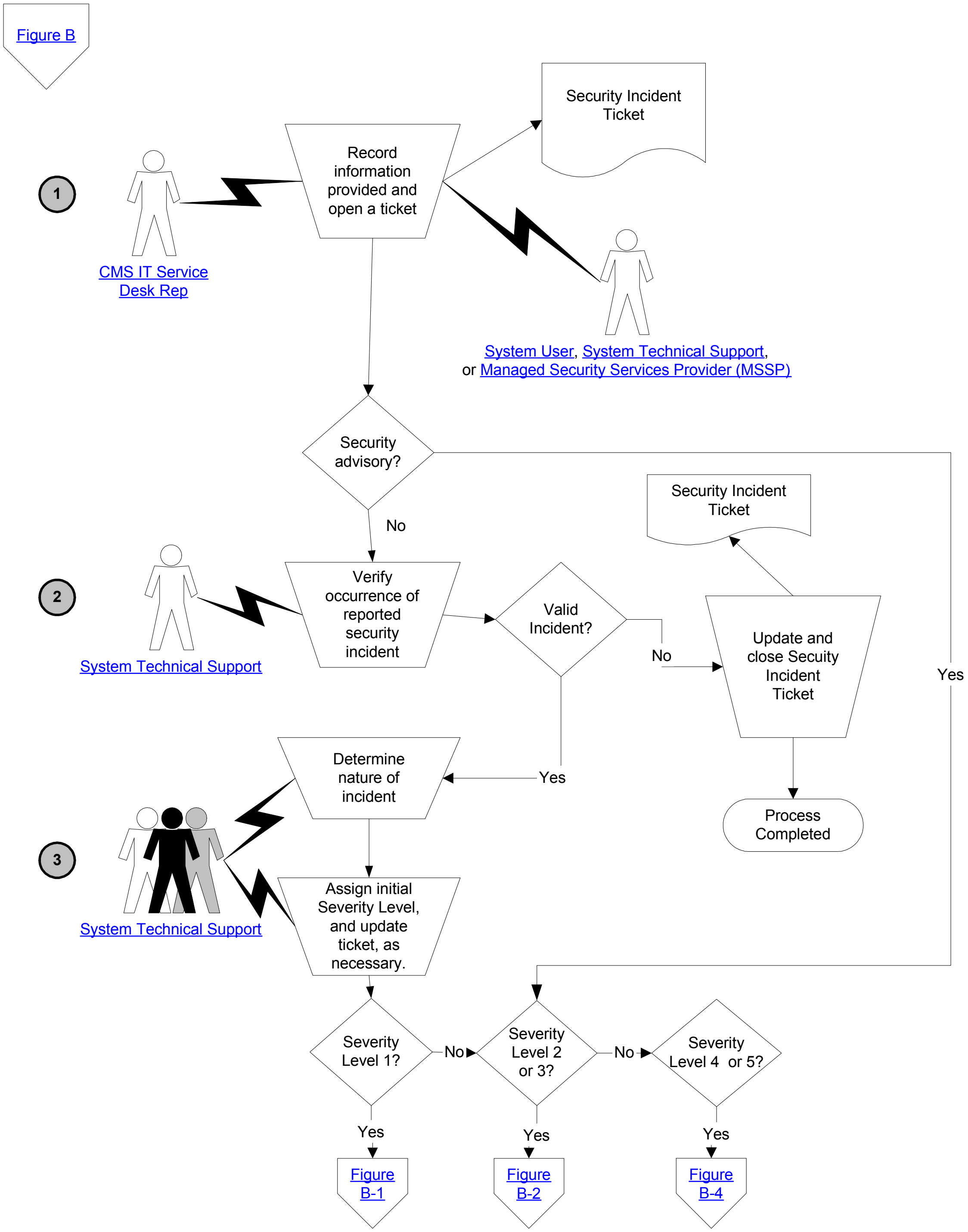
Figure B
1
CMS IT Service Desk Rep
Record information provided and open a ticket
Security Incident Ticket
System User, System Technical Support, or Managed Security Services Provider (MSSP)
Security advisory?
No
Yes
2
System Technical Support
Verify occurrence of reported security incident
Valid Incident?
No
Security Incident Ticket
Update and close Secuity Incident Ticket
Process Completed
Yes
3
System Technical Support
Determine nature of incident
Assign initial Severity Level, and update ticket, as necessary.
Severity Level 1?
No
Severity Level 2 or 3?
No
Severity Level 4 or 5?
Yes
Yes
Yes
Figure B-1
Figure B-2
Figure B-4

# System Security Incident Handling Action Step
# Severity Level 1

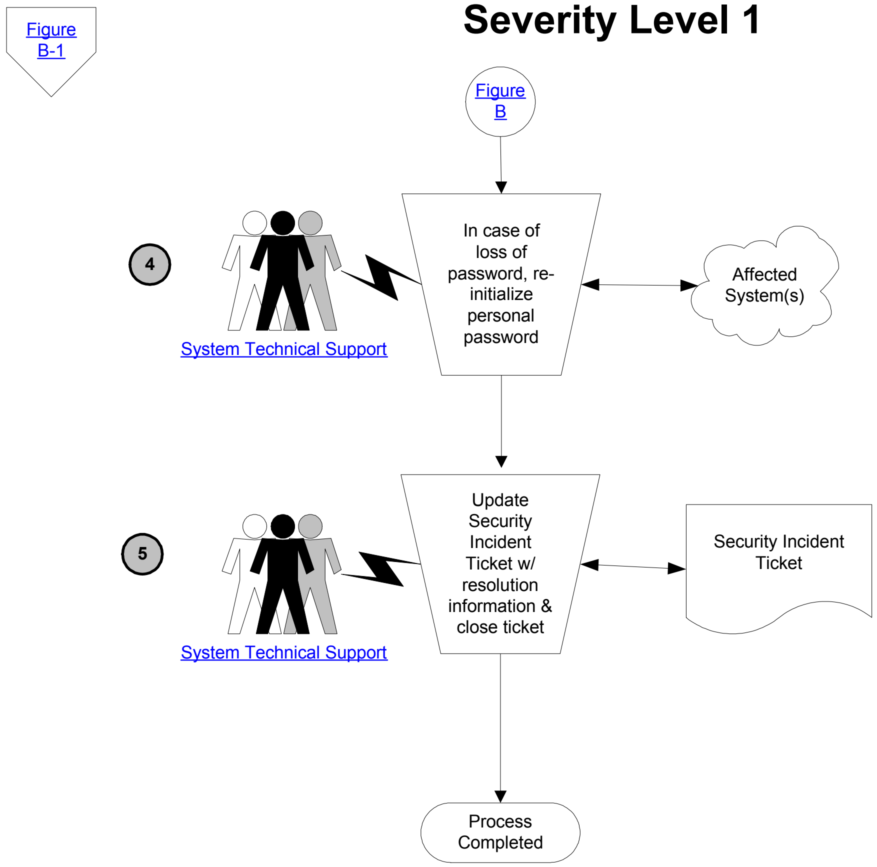
Figure B-1
Figure B
4
System Technical Support
In case of loss of password, re-initialize personal password
Affected System(s)
5
System Technical Support
Update Security Incident Ticket w/ resolution information & close ticket
Security Incident Ticket
Process Completed

# System Security Incident Handling Action Steps
# Severity Level 2 or 3

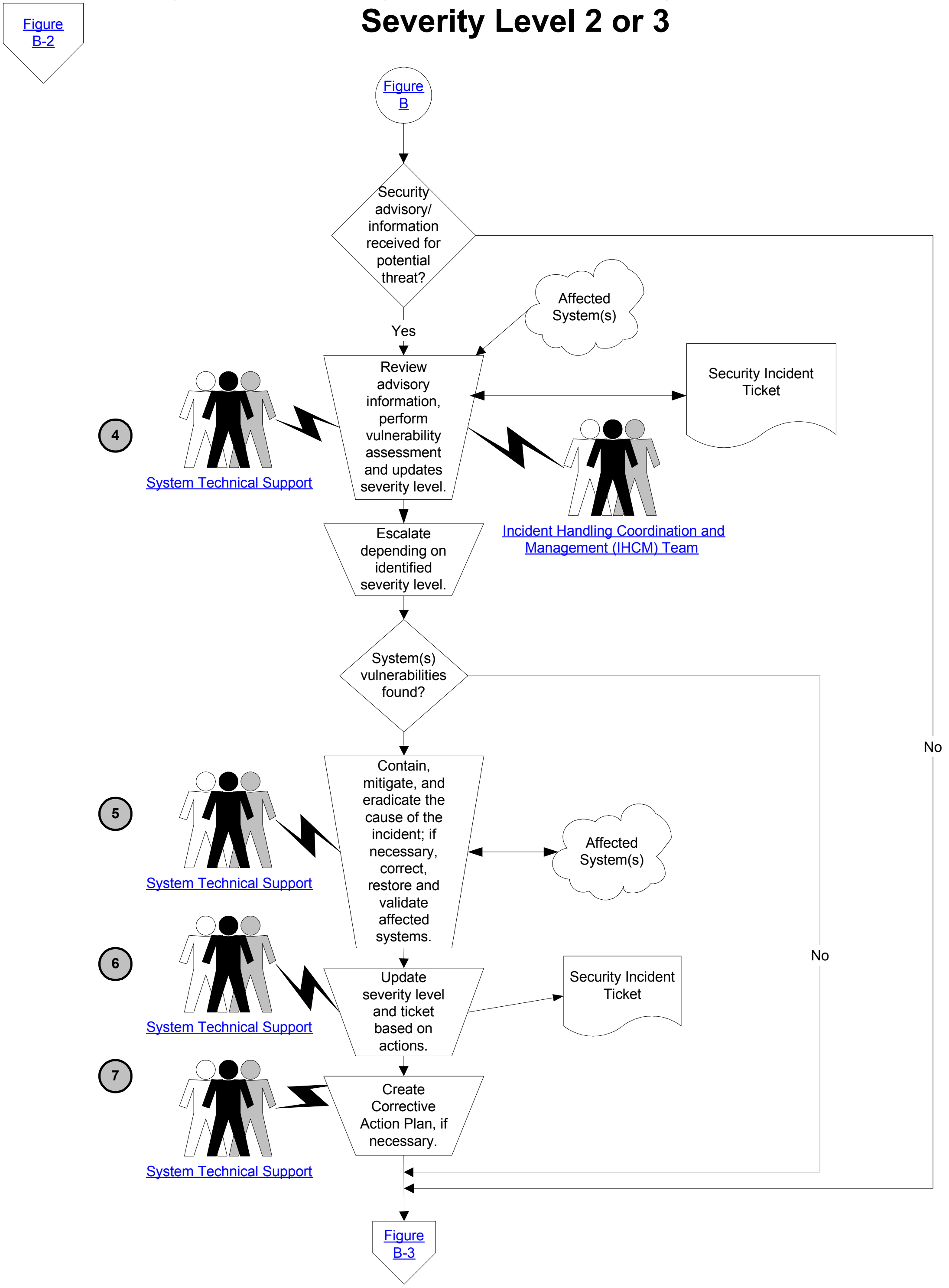
Figure B-2
Figure B
Security advisory/ information received for potential threat?
Yes
No
Affected System(s)
Review advisory information, perform vulnerability assessment and updates severity level.
Security Incident Ticket
4
System Technical Support
Incident Handling Coordination and Management (IHCM) Team
Escalate depending on identified severity level.
System(s) vulnerabilities found?
No
5
System Technical Support
Contain, mitigate, and eradicate the cause of the incident; if necessary, correct, restore and validate affected systems.
Affected System(s)
6
System Technical Support
Update severity level and ticket based on actions.
Security Incident Ticket
7
System Technical Support
Create Corrective Action Plan, if necessary.
Figure B-3

## System Security Incident Handling Action Steps Severity Level 2 or 3 (Continued)

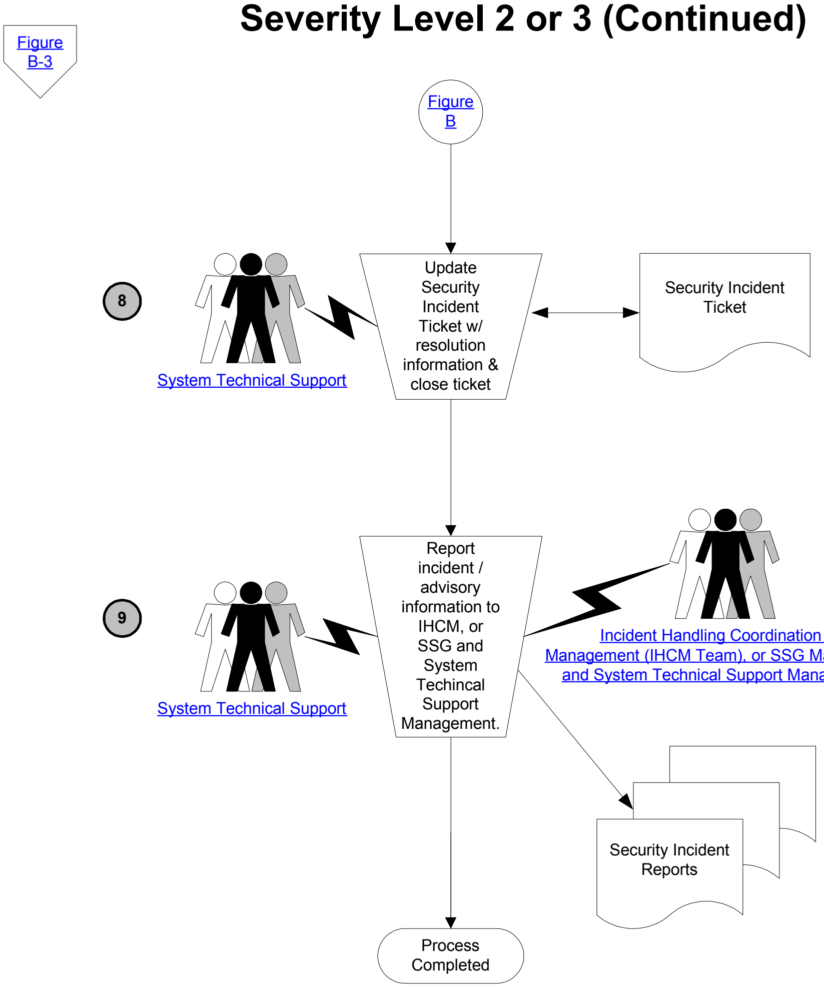
Figure B-3
Figure B
8
System Technical Support
Update Security Incident Ticket w/ resolution information & close ticket
Security Incident Ticket
9
System Technical Support
Report incident / advisory information to IHCM, or SSG and System Techincal Support Management.
Incident Handling Coordination and Management (IHCM Team), or SSG Management and System Technical Support Management.
Security Incident Reports
Process Completed

Figure B-4

# System Security Incident Handling Action Steps
# Severity Level 4 or 5

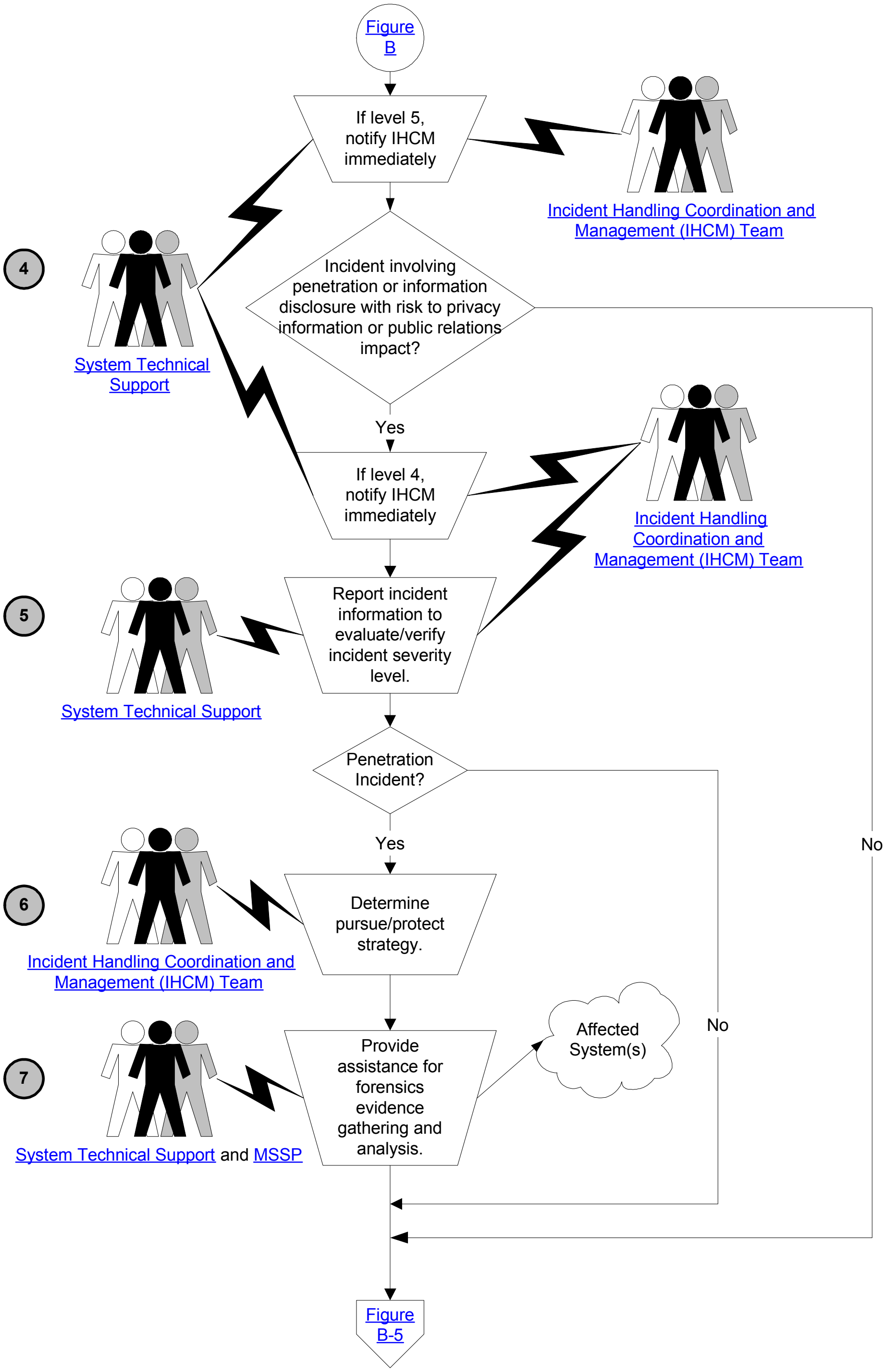
Figure B
If level 5, notify IHCM immediately
Incident Handling Coordination and Management (IHCM) Team
4
System Technical Support
Incident involving penetration or information disclosure with risk to privacy information or public relations impact?
Yes
No
If level 4, notify IHCM immediately
Incident Handling Coordination and Management (IHCM) Team
5
Report incident information to evaluate/verify incident severity level.
System Technical Support
Penetration Incident?
Yes
No
6
Determine pursue/protect strategy.
Incident Handling Coordination and Management (IHCM) Team
7
Provide assistance for forensics evidence gathering and analysis.
Affected System(s)
System Technical Support and MSSP
Figure B-5

Figure B-5

# System Security Incident Handling Action Steps Severity Level 4 or 5 (Continued)

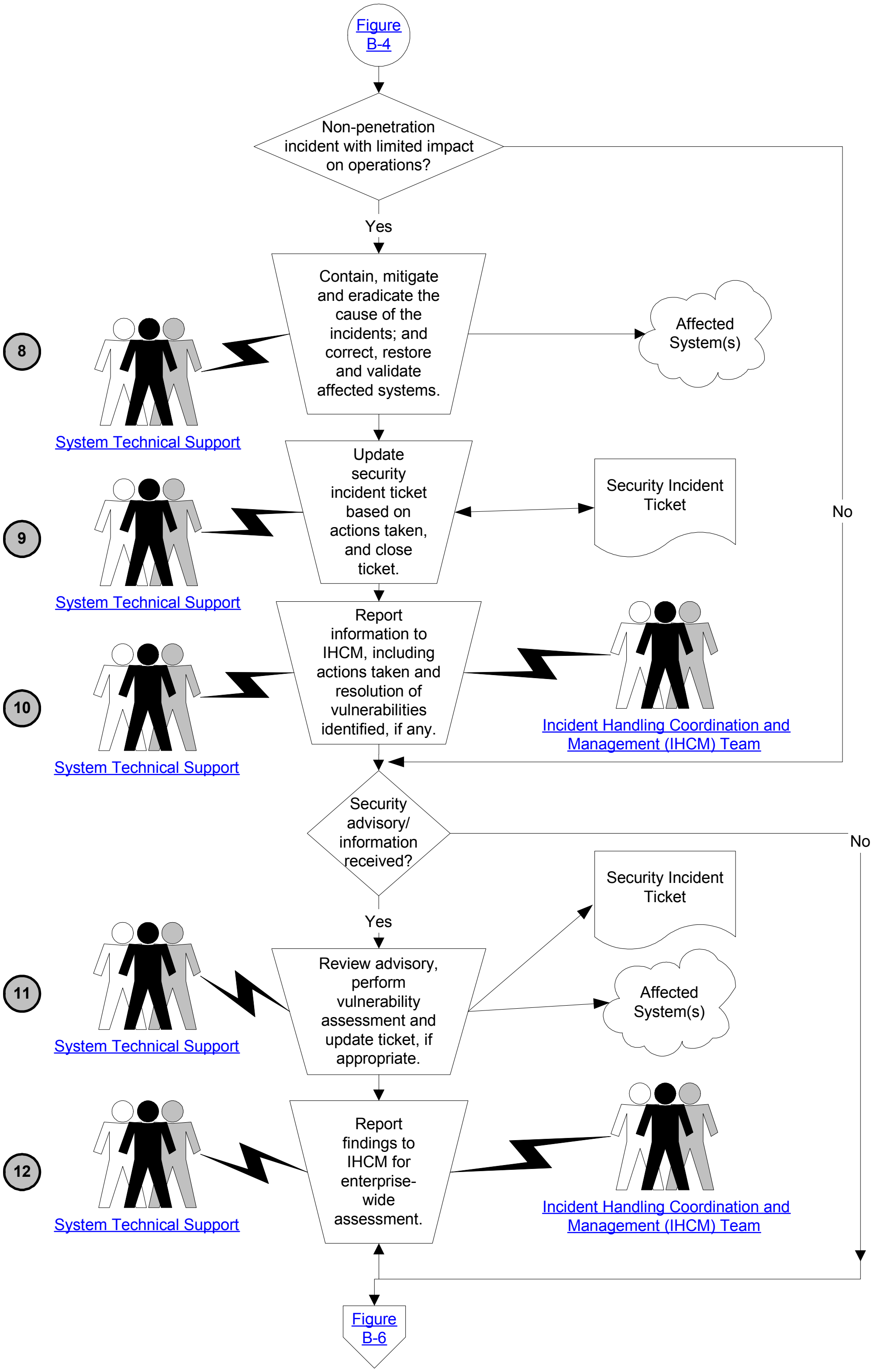
Figure B-4
Non-penetration incident with limited impact on operations?
Yes
No
8
Contain, mitigate and eradicate the cause of the incidents; and correct, restore and validate affected systems.
Affected System(s)
System Technical Support
9
Update security incident ticket based on actions taken, and close ticket.
Security Incident Ticket
System Technical Support
10
Report information to IHCM, including actions taken and resolution of vulnerabilities identified, if any.
Incident Handling Coordination and Management (IHCM) Team
System Technical Support
Security advisory/ information received?
No
Yes
Security Incident Ticket
11
Review advisory, perform vulnerability assessment and update ticket, if appropriate.
Affected System(s)
System Technical Support
12
Report findings to IHCM for enterprise-wide assessment.
Incident Handling Coordination and Management (IHCM) Team
System Technical Support
Figure B-6

# System Security Incident Handling Action Steps
# Severity Level 4 or 5 (Continued)

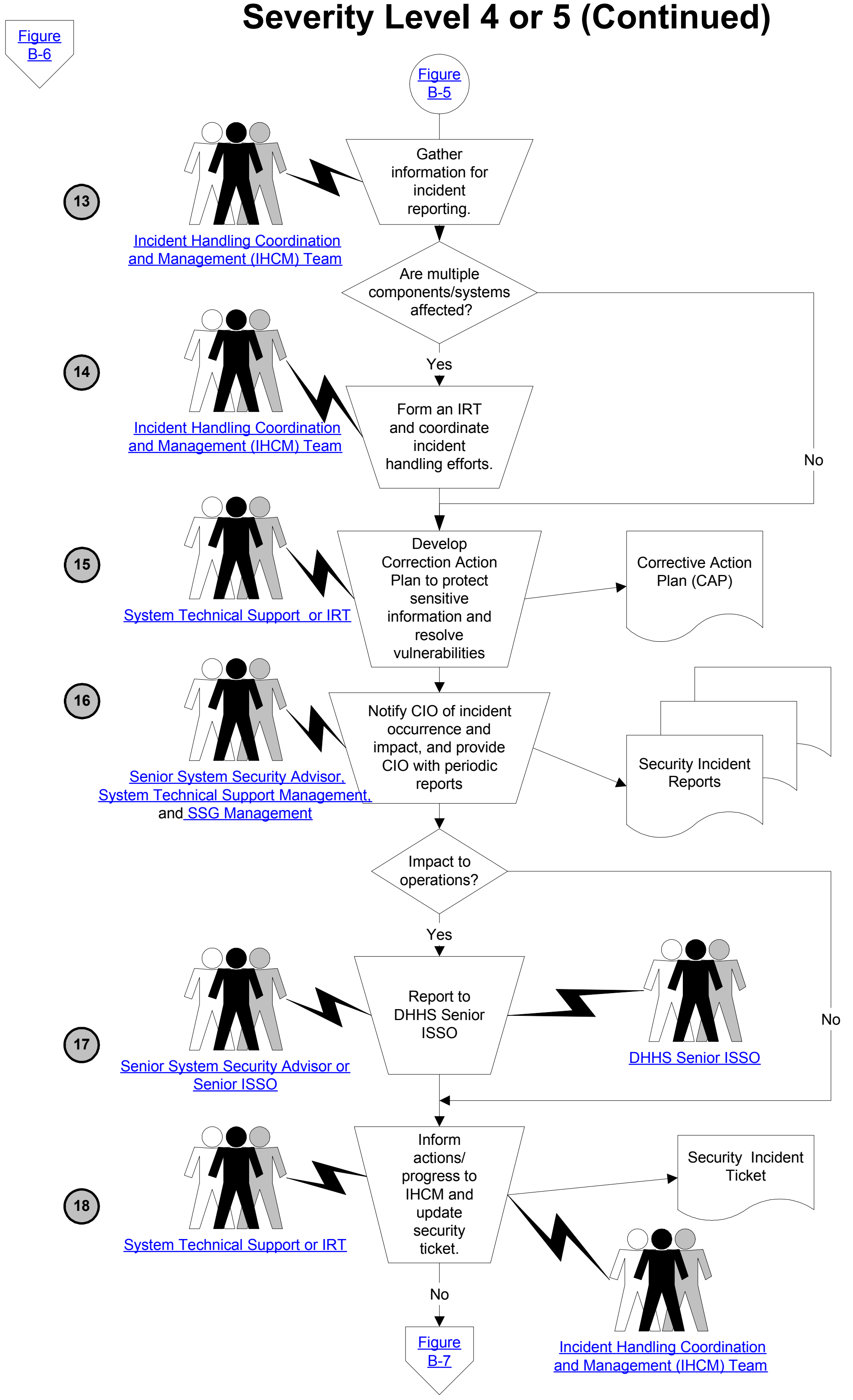
Figure B-6
Figure B-5
13
Incident Handling Coordination and Management (IHCM) Team
Gather information for incident reporting.
Are multiple components/systems affected?
Yes
No
14
Incident Handling Coordination and Management (IHCM) Team
Form an IRT and coordinate incident handling efforts.
15
System Technical Support or IRT
Develop Correction Action Plan to protect sensitive information and resolve vulnerabilities
Corrective Action Plan (CAP)
16
Senior System Security Advisor, System Technical Support Management, and SSG Management
Notify CIO of incident occurrence and impact, and provide CIO with periodic reports
Security Incident Reports
Impact to operations?
Yes
No
17
Senior System Security Advisor or Senior ISSO
Report to DHHS Senior ISSO
DHHS Senior ISSO
18
System Technical Support or IRT
Inform actions/ progress to IHCM and update security ticket.
Security Incident Ticket
Incident Handling Coordination and Management (IHCM) Team
No
Figure B-7

# System Security Incident Handling Action Steps
# Severity Level 4 or 5 (Continued)

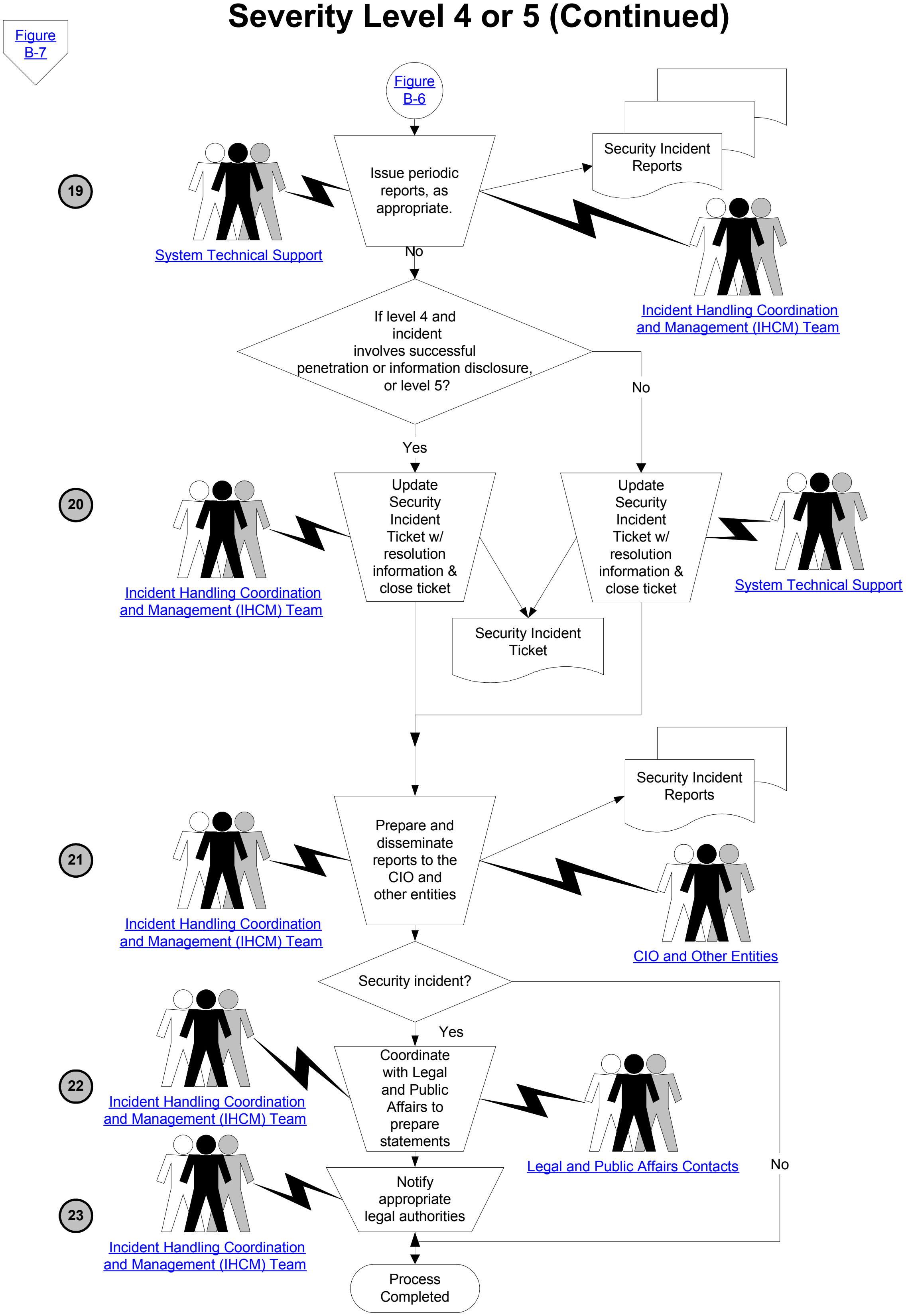
Figure B-7
Figure B-6
19
Issue periodic reports, as appropriate.
Security Incident Reports
System Technical Support
Incident Handling Coordination and Management (IHCM) Team
No
If level 4 and incident involves successful penetration or information disclosure, or level 5?
No
Yes
20
Update Security Incident Ticket w/ resolution information & close ticket
Update Security Incident Ticket w/ resolution information & close ticket
Incident Handling Coordination and Management (IHCM) Team
System Technical Support
Security Incident Ticket
Security Incident Reports
21
Prepare and disseminate reports to the CIO and other entities
Incident Handling Coordination and Management (IHCM) Team
CIO and Other Entities
Security incident?
Yes
22
Coordinate with Legal and Public Affairs to prepare statements
Incident Handling Coordination and Management (IHCM) Team
Legal and Public Affairs Contacts
No
23
Notify appropriate legal authorities
Incident Handling Coordination and Management (IHCM) Team
Process Completed

## Appendix C – References

CMS Information System Security Policy, Standards and Guidelines Handbook
http://cms.hhs.gov/it/security/docs/handbook.pdf

HHS IRM Policy for Establishing an Incident Response Capability
http://www.hhs.gov/read/irmpolicy/0006.html